Official website of the Department of Homeland Security

NICCS™

National Initiative for Cybersecurity Careers and Studies

The NICCS glossary contains key cybersecurity terms that enable clear communication and a common understanding of cybersecurity definitions.

Explore Terms: A Glossary of Common Cybersecurity Terminology

The NICCS Portal’s cybersecurity lexicon is intended to serve the cybersecurity communities of practice and interest for both the public and private sectors. It complements other lexicons such as the NISTIR 7298 Glossary of Key Information Security Terms. Objectives for lexicon are to enable clearer communication and common understanding of cybersecurity terms, through use of plain English and annotations on the definitions. The lexicon will evolve through ongoing feedback from end users and stakeholders.

Acronyms

A

access

Definition: The ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

From: CNSSI 4009

access and identity management

Synonym(s): identity and access management

access control

Definition: The process of granting or denying specific requests for or attempts to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities.

Related Term(s): access control mechanism

Adapted from: CNSSI 4009

access control mechanism

Definition: Security measures designed to detect and deny unauthorized access and permit authorized access to an information system or a physical facility.

Adapted from: CNSSI 4009

active attack

Definition: An actual assault perpetrated by an intentional threat source that attempts to alter a system, its resources, its data, or its operations.

Related Term(s): passive attack

Adapted from: IETF RFC 4949, NIST SP 800-63 Rev 1

active content

Definition: Software that is able to automatically carry out or trigger actions without the explicit intervention of a user.

Adapted from: CNSSI 4009

Advanced Persistent Threat

Definition: An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

From: NIST SP 800-53 Rev 4

adversary

Definition: An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Related Term(s): threat agent, attacker

From: DHS Risk Lexicon

air gap

Definition: To physically separate or isolate a system from other systems or networks (verb).

Extended Definition: The physical separation or isolation of a system from other systems or networks (noun).

alert

Definition: A notification that a specific attack has been detected or directed at an organization’s information systems.

Adapted from: CNSSI 4009

All Source Intelligence

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.

From: NICE Workforce Framework

Analyze

Definition: A NICE Workforce Framework category consisting of specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

From: NICE Workforce Framework

antispyware software

Definition: A program that specializes in detecting and blocking or removing forms of spyware.

Related Term(s): spyware

Adapted from: NCSD Glossary

antivirus software

Definition: A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents. Sometimes by removing or neutralizing the malicious code.

Adapted from: NCSD Glossary

asset

Definition: A person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value.

Extended Definition: Anything useful that contributes to the success of something, such as an organizational mission; assets are things of value or properties to which value can be assigned.

Adapted from: DHS Risk Lexicon

asymmetric cryptography

Synonym(s): public key cryptography

attack

Definition: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

Extended Definition: The intentional act of attempting to bypass one or more security services or controls of an information system.

Related Term(s): active attack, passive attack

From: NCSD Glossary. NTSSI 4009 (2000), CNSSI 4009

attack method

Definition: The manner or technique and means an adversary may use in an assault on information or an information system.

Adapted from: DHS Risk Lexicon, NCSD Glossary

attack mode

Synonym(s): attack method

attack path

Definition: The steps that an adversary takes or may take to plan, prepare for, and execute an attack.

Adapted from: DHS Risk Lexicon, NCSD Glossary

attack pattern

Definition: Similar cyber events or behaviors that may indicate an attack has occurred or is occurring, resulting in a security violation or a potential security violation.

Extended Definition: For software, descriptions of common methods for exploiting software systems.

Related Term(s): attack signature

Adapted from: Oak Ridge National Laboratory Visualization Techniques for Computer Network Defense, MITRE's CAPEC web site

attack signature

Definition: A characteristic or distinctive pattern that can be searched for or that can be used in matching to previously identified attacks.

Extended Definition: An automated set of rules for identifying a potential threat (such as an exploit or the presence of an attacker tool) and possible responses to that threat.

Related Term(s): attack pattern

Adapted from: NCSD Glossary, CNSSI 4009, ISSG V1.2 Database

attack surface

Definition: The set of ways in which an adversary can enter a system and potentially cause damage.

Extended Definition: An information system's characteristics that permit an adversary to probe, attack, or maintain presence in the information system.

Adapted from: Manadhata, P.K., & Wing, J.M. in Attack Surface Measurement; DHS personnel

attacker

Definition: An individual, group, organization, or government that executes an attack.

Extended Definition: A party acting with malicious intent to compromise an information system.

Related Term(s): adversary, threat agent

Adapted from: Barnum & Sethi (2006), NIST SP 800-63 Rev 1

authenticate

Related Term(s): authentication

authentication

Definition: The process of verifying the identity or other attributes of an entity (user, process, or device).

Extended Definition: Also the process of verifying the source and integrity of data.

Adapted from: CNSSI 4009, NIST SP 800-21, NISTIR 7298

authenticity

Definition: A property achieved through cryptographic methods of being genuine and being able to be verified and trusted, resulting in confidence in the validity of a transmission, information or a message, or sender of information or a message.

Related Term(s): integrity, non-repudiation

Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4

authorization

Definition: A process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource.

Extended Definition: The process or act of granting access privileges or the access

privileges as granted.

From: OASIS SAML Glossary 2.0; Adapted from CNSSI 4009

availability

Definition: The property of being accessible and usable upon demand.

Extended Definition: In cybersecurity, applies to assets such as information or information systems.

Related Term(s): confidentiality, integrity

Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, 44 U.S.C., Sec 3542

B

behavior monitoring

Definition: Observing activities of users, information systems, and processes and measuring the activities against organizational policies and rule, baselines of normal activity, thresholds, and trends.

Adapted from: DHS personnel

behavioral monitoring

Synonym(s): behavior monitoring

blacklist

Definition: A list of entities that are blocked or denied privileges or access.

Related Term(s): whitelist

Adapted from: DHS personnel

Blue Team

Definition: A group that defends an enterprise's information systems when mock attackers (i.e., the Red Team) attack, typically as part of an operational exercise conducted according to rules established and monitored by a neutral group (i.e., the White Team).

Extended Definition: Also, a group that conducts operational vulnerability evaluations and recommends mitigation techniques to customers who need an independent technical review of their cybersecurity posture.

Related Term(s): Red Team, White Team

Adapted from: CNSSI 4009

bot

Definition: A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under remote the

command and control of a remote administrator.

Extended Definition: A member of a larger collection of compromised computers known as a botnet.

Synonym(s): zombie

Related Term(s): botnet

bot herder

Synonym(s): bot master

bot master

Definition: The controller of a botnet that, from a remote location, provides direction to the compromised computers in the botnet.

Synonym(s): bot herder

botnet

Definition: A collection of computers compromised by malicious code and controlled across a network.

bug

Definition: An unexpected and relatively small defect, fault, flaw, or imperfection in an

information system or device.

Adapted from: NCSD Glossary

Build Security In

Definition: A set of principles, practices, and tools to design, develop, and evolve information systems and software that enhance resistance to vulnerabilities, flaws, and attacks.

Adapted from: Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program (2011), US-CERT's Build Security In website.

C

capability

Definition: The means to accomplish a mission, function, or objective.

Related Term(s): intent

Adapted from: DHS Risk Lexicon

cipher

Synonym(s): cryptographic algorithm

ciphertext

Definition: Data or information in its encrypted form.

Related Term(s): plaintext

From: CNSSI 4009

cloud computing

Definition: A model for enabling on-demand network access to a shared pool of configurable computing capabilities or resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Adapted from: CNSSI 4009, NIST SP 800-145

Collect & Operate

Definition: A NICE Workforce Framework category consisting of specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

From: NICE Workforce Framework

Collection Operations

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Executes collection using appropriate strategies and within the priorities established

through the collection management process.

From: NICE Workforce Framework

computer forensics

Synonym(s): digital forensics

computer network defense

Definition: The actions taken to defend against unauthorized activity within computer networks.

From: CNSSI 4009

Computer Network Defense Analysis

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

From: NICE Workforce Framework

Computer Network Defense Infrastructure Support

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Tests, implements, deploys, maintains, reviews, and administers the infrastructure

hardware and software that are required to effectively manage the computer network defense service provider network and resources; monitors network to actively remediate unauthorized activities.

From: NICE Workforce Framework

computer security incident

Synonym(s): incident

Related Term(s): event

confidentiality

Definition: A property that information is not disclosed to users, processes, or devices unless they have been authorized to access the information.

Extended Definition: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Related Term(s): availability, integrity

Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, 44 U.S.C., Sec 3542

consequence

Definition: The effect of an event, incident, or occurrence.

Extended Definition: In cybersecurity, the effect of a loss of confidentiality, integrity or availability of information or an information system on an organization's operations, its assets, on individuals, other organizations, or on national interests.

Adapted from: DHS Risk Lexicon, National Infrastructure Protection Plan, NIST SP 800-53 Rev 4

Continuity of Operations Plan

Definition: A document that sets forth procedures for the continued performance of core capabilities and critical operations during any disruption or potential disruption.

Related Term(s): Business Continuity Plan, Disaster Recovery Plan, Contingency Plan

Adapted from: CPG 101, CNSSI 4009

critical infrastructure

Definition: The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.

Related Term(s): key resource

Adapted from: National Infrastructure Protection Plan

critical infrastructure and key resources

Synonym(s): critical infrastructure

cryptanalysis

Definition: The operations performed in defeating or circumventing cryptographic protection of information by applying mathematical techniques and without an initial knowledge of the key employed in providing the protection.

Extended Definition: The study of mathematical techniques for attempting to defeat or circumvent cryptographic techniques and/or information systems security.

Adapted from: CNSSI 4009, NIST SP 800-130

cryptographic algorithm

Definition: A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output.

Related Term(s): key, encryption, decryption, symmetric key, asymmetric key

From: CNSSI 4009

cryptography

Definition: The use of mathematical techniques to provide security services, such as confidentiality, data integrity, entity authentication, and data origin authentication.

Extended Definition: The art or science concerning the principles, means, and methods for converting plaintext into ciphertext and for restoring encrypted ciphertext to plaintext.

Related Term(s): plaintext, ciphertext, encryption, decryption

From: NIST SP 800-130; Adapted from: CNSSI 4009

cryptology

Definition: The mathematical science that deals with cryptanalysis and cryptography.

Related Term(s): cryptanalysis, cryptography

From: CNSSI 4009

Customer Service and Technical Support

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Addresses problems, installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

From: NICE Workforce Framework

cyber ecosystem

Definition: The interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions.

Adapted from: DHS personnel

cyber exercise

Definition: A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption.

Adapted from: NCSD Glossary, DHS Homeland Security Exercise and Evaluation Program

cyber incident

Synonym(s): incident

Related Term(s): event

cyber incident response plan

Synonym(s): incident response plan

cyber infrastructure

Definition: An electronic information and communications systems and services and the information contained therein.

Extended Definition: The information and communications systems and services composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements: • Processing includes the creation, access, modification, and destruction of information. • Storage includes paper, magnetic, electronic, and all other media types. • Communications include sharing and distribution of information.

Adapted from: NIPP

Cyber Operations

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.

From: NICE Workforce Framework

Cyber Operations Planning

Definition: in the NICE Workforce Framework, cybersecurity work where a person: Performs in-depth joint targeting and cyber planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations

From: NICE Workforce Framework

cybersecurity

Definition: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Extended Definition: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009

cyberspace

Definition: The interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Adapted from: NSPD 54/HSPD -23, CNSSI 4009, NIST SP 800-53 Rev 4

D

Data Administration

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

From: NICE Workforce Framework

data aggregation

Definition: The process of gathering and combining data from different sources, so that the combined data reveals new information.

Extended Definition: The new information is more sensitive than the individual data elements themselves and the person who aggregates the data was not granted access to the totality of the information.

Related Term(s): data mining

Adapted from: CNSSI 4009

data breach

Definition: The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

Related Term(s): data loss, data theft, exfiltration

data integrity

Definition: The property that data is complete, intact, and trusted and has not been modified or destroyed in an unauthorized or accidental manner.

Related Term(s): integrity, system integrity

Adapted from: CNSSI 4009, NIST SP 800-27

data leakage

Synonym(s): data breach

data loss

Definition: The result of unintentionally or accidentally deleting data, forgetting where it is stored, or exposure to an unauthorized party.

Related Term(s): data leakage, data theft

data loss prevention

Definition: A set of procedures and mechanisms to stop sensitive data from leaving a security boundary.

Related Term(s): data loss, data theft, data leak

Adapted from: Liu, S., & Kuhn, R. (2010, March/April). Data loss prevention. IEEE IT Professional, 11(2), pp. 10-13.

data mining

Definition: The process or techniques used to analyze large sets of existing information to discover previously unrevealed patterns or correlations.

Related Term(s): data aggregation

Adapted from: DHS personnel

data spill

Synonym(s): data breach

data theft

Definition: The deliberate or intentional act of stealing of information.

Related Term(s): data aggregation, data leakage, data loss

decipher

Definition: To convert enciphered text to plain text by means of a cryptographic system.

Synonym(s): decode, decrypt

From: CNSSI 4009

decode

Definition: To convert encoded text to plain text by means of a code.

Synonym(s): decipher, decrypt

From: CNSSI 4009

decrypt

Definition: A generic term encompassing decode and decipher.

Synonym(s): decipher, decode

From: CNSSI 4009

decryption

Definition: The process of transforming ciphertext into its original plaintext.

Extended Definition: The process of converting encrypted data back into its original form, so it can be understood.

Synonym(s): decode, decrypt, decipher

Adapted from: ICAM SAML 2.0 WB SSO Profile 1.0.2

denial of service

Definition: An attack that prevents or impairs the authorized use of information system resources or services.

Adapted from: NCSD Glossary

designed-in security

Synonym(s): Build Security In

digital forensics

Definition: The processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes.

Extended Definition: In the NICE Workforce Framework, cybersecurity work where a person: Collects, processes, preserves, analyzes, and presents computer-related

evidence in support of network vulnerability, mitigation, and/or criminal, fraud, counterintelligence or law enforcement investigations.

Synonym(s): computer forensics, forensics

Adapted from: CNSSI 4009; From: NICE Workforce Framework

digital rights management

Definition: A form of access control technology to protect and manage use of digital content or devices in accordance with the content or device provider's intentions.

digital signature

Definition: A value computed with a cryptographic process using a private key and then appended to a data object, thereby digitally signing the data.

Related Term(s): electronic signature

Adapted from: CNSSI 4009, IETF RFC 2828, ICAM SAML 2.0 WB SSO Profile 1.0.2, InCommon Glossary, NIST SP 800-63 Rev 1

disruption

Definition: An event which causes unplanned interruption in operations or functions for an unacceptable length of time.

Adapted from: CNSSI 4009

distributed denial of service

Definition: A denial of service technique that uses numerous systems to perform the attack simultaneously.

Related Term(s): denial of service, botnet

Adapted from: CNSSI 4009

dynamic attack surface

Definition: The automated, on-the-fly changes of an information system's characteristics to thwart actions of an adversary.

Adapted from: DHS personnel

E

Education and Training

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Conducts training of personnel within pertinent subject domain; develop, plan, coordinate, deliver, and/or evaluate training courses, methods, and techniques as appropriate.

From: NICE Workforce Framework

electronic signature

Definition: Any mark in electronic form associated with an electronic document, applied with the intent to sign the document.

Related Term(s): digital signature

Adapted from: CNSSI 4009

encipher

Definition: To convert plaintext to ciphertext by means of a cryptographic system.

Synonym(s): encode, encrypt

From: CNSSI 4009

encode

Definition: To convert plaintext to ciphertext by means of a code.

Synonym(s): encipher, encrypt

From: CNSSI 4009

encrypt

Definition: The generic term encompassing encipher and encode.

Synonym(s): encipher, encode

From: CNSSI 4009

encryption
Definition: The process of transforming plaintext into ciphertext.

Extended Definition: Converting data into a form that cannot be easily understood by unauthorized people.

Synonym(s): encode, encrypt, encipher

Adapted from: CNSSI 4009, ICAM SAML 2.0 WB SSO Profile 1.0.2

enterprise risk management
Definition: A comprehensive approach to risk management that engages people, processes, and systems across an organization to improve the quality of decision making for managing risks that may hinder an organization’s ability to achieve its objectives.

Extended Definition: Involves identifying mission dependencies on enterprise capabilities, identifying and prioritizing risks due to defined threats, implementing countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and assessing enterprise performance against threats and adjusts countermeasures as necessary.

Related Term(s): risk management, integrated risk management, risk

Adapted from: DHS Risk Lexicon, CNSSI 4009

event

Definition: An observable occurrence in an information system or network.

Extended Definition: Sometimes provides an indication that an incident is occurring or at least raise the suspicion that an incident may be occurring.

Related Term(s): incident

Adapted from: CNSSI 4009

exfiltration

Definition: The unauthorized transfer of information from an information system.

Related Term(s): data breach

From: NIST SP 800-53 Rev 4

exploit

Definition: A technique to breach the security of a network or information system in violation of security policy.

Adapted from: ISO/IEC 27039 (draft), DHS personnel

Exploitation Analysis

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Analyzes collected information to identify vulnerabilities and potential for exploitation.

From: NICE Workforce Framework

exposure

Definition: The condition of being unprotected, thereby allowing access to information or access to capabilities that an attacker can use to enter a system or network.

Adapted from: NCSD glossary

F

Failure

Definition: The inability of a system or component to perform its required functions within specified performance requirements.

From: NCSD Glossary

firewall

Definition: A capability to limit network traffic between networks and/or information systems.

Extended Definition: A hardware/software device or a software program that limits network traffic according to a set of rules of what access is and is not allowed or authorized.

Adapted from: CNSSI 4009

forensics

Synonym(s): digital forensics

G

H

hacker

Definition: An unauthorized user who attempts to or gains access to an information system.

From: CNSSI 4009

hash value

Definition: A numeric value resulting from applying a mathematical algorithm against a set of data such as a file.

Synonym(s): cryptographic hash value

Related Term(s): hashing

Adapted from: CNSSI 4009

hashing

Definition: A process of applying a mathematical algorithm against a set of data to produce a numeric value (a 'hash value') that represents the data.

Extended Definition: Mapping a bit string of arbitrary length to a fixed length bit string to produce the hash value.

Related Term(s): hash value

Adapted from: CNSSI 4009, FIPS 201-2

hazard

Definition: A natural or man-made source or cause of harm or difficulty.

Related Term(s): threat

From: DHS Risk Lexicon

I

ICT supply chain threat

Definition: A man-made threat achieved through exploitation of the information and communications technology (ICT) system’s supply chain, including acquisition processes.

Related Term(s): supply chain, threat

From: DHS SCRM PMO

identity and access management

Definition: The methods and processes used to manage subjects and their authentication and authorizations to access specific objects.

impact

Synonym(s): consequence

incident

Definition: An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

Extended Definition: An occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Related Term(s): event

Adapted from: CNSSI 4009, FIPS 200, NIST SP 800-53 Rev 4, ISSG

incident management

Definition: The management and coordination of activities associated with an actual or potential occurrence of an event that may result in adverse consequences to information or information systems.

Adapted from: NCSD Glossary, ISSG NCPS Target Architecture Glossary

incident response

Definition: The activities that address the short-term, direct effects of an incident and may also support short-term recovery.

Extended Definition: In the Workforce framework, cybersecurity work where a person: Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats; uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

Synonym(s): response

Related Term(s): recovery

From: Workforce Framework

incident response plan
Definition: A set of predetermined and documented procedures to detect and respond to a cyber incident.

Adapted from: CNSSI 4009

indicator
Definition: An occurrence or sign that an incident may have occurred or may be in progress.

Related Term(s): precursor

Adapted from: CNSSI 4009, NIST SP 800-61 Rev 2 (DRAFT), ISSG V1.2 Database

Industrial Control System
Definition: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution or to control infrastructure assets.

Related Term(s): Supervisory Control and Data Acquisition, Operations Technology

Adapted from: NIST SP 800-53 Rev 4, NIST SP 800-82

information and communication(s) technology

Definition: Any information technology, equipment, or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.

Related Term(s): information technology

Adapted from: The Access Board's 2011 Advance Notice of Proposed Rulemaking for Section 508

information assurance

Definition: The measures that protect and defend information and information systems by ensuring their availability, integrity, and confidentiality.

Related Term(s): information security

Adapted from: CNSSI 4009

Information Assurance Compliance

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's information assurance and security requirements; ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

From: NICE Workforce Framework

information security policy

Definition: An aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.

Related Term(s): security policy

From: CNSSI 4009; NIST SP 800-53 Rev 4

information sharing

Definition: An exchange of data, information, and/or knowledge to manage risks or respond to incidents.

Adapted from: NCSD glossary

information system resilience

Definition: The ability of an information system to: (1) continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while

maintaining essential operational capabilities; and (2) recover effectively in a timely manner.

Related Term(s): resilience

Adapted from: NIST SP 800-53 Rev 4

Information Systems Security Operations

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Oversees the information assurance program of an information system in or outside the network environment; may include procurement duties (e.g., Information Systems Security Officer).

From: NICE Workforce Framework

information technology

Definition: Any equipment or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.

Related Term(s): information and communication(s) technology

Adapted from: CNSSI 4009, NIST SP 800-53 rev. 4, based on 40 U.S.C. sec. 1401

inside(r) threat

Definition: A person or group of persons within an organization who pose a potential

risk through violating security policies.

Extended Definition: One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.

Related Term(s): outside(r) threat

Adapted from: CNSSI 4009; From: NIAC Final Report and Recommendations on the Insider Threat to Critical Infrastructure, 2008

integrated risk management

Definition: The structured approach that enables an enterprise or organization to share risk information and risk analysis and to synchronize independent yet complementary risk management strategies to unify efforts across the enterprise.

Related Term(s): risk management, enterprise risk management

Adapted from: DHS Risk Lexicon

integrity

Definition: The property whereby information, an information system, or a component of a system has not been modified or destroyed in an unauthorized manner.

Extended Definition: A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

Related Term(s): availability, confidentiality, data integrity, system integrity

Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, 44 U.S.C., Sec 3542, SANS; From SAFE-BioPharma Certificate Policy 2.5

intent

Definition: A state of mind or desire to achieve an objective.

Related Term(s): capability

Adapted from: DHS Risk Lexicon

interoperability

Definition: The ability of two or more systems or components to exchange information and to use the information that has been exchanged.

Adapted from: IEEE Standard Computer Dictionary, DHS personnel

intrusion

Definition: An unauthorized act of bypassing the security mechanisms of a network or information system.

Synonym(s): penetration

Adapted from: CNSSI 4009

intrusion detection

Definition: The process and methods for analyzing information from networks and information systems to determine if a security breach or security violation has occurred.

Adapted from: CNSSI 4009, ISO/IEC 27039 (draft)

Investigate

Definition: a NICE Workforce Framework category consisting of specialty areas responsible for the investigation of cyber events and/or crimes of IT systems, networks, and digital evidence

From: NICE Workforce Framework

investigation

Definition: A systematic and formal inquiry into a qualified threat or incident using digital forensics and perhaps other traditional criminal inquiry techniques to determine the events that transpired and to collect evidence.

Extended Definition: In the NICE Workforce Framework, cybersecurity work where a person: Applies tactics, techniques, and procedures for a full range of investigative

tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

Adapted from: ISSG V1.2 Database; Conrad, E., Misenauer, S., & Feldman, J. (2010). CISSP® Study Guide. Burlington, MA: Syngress; From: NICE Workforce Framework

IT asset

Synonym(s): asset

J

K

key

Definition: The numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

Related Term(s): private key, public key, secret key, symmetric key

From: CNSSI 4009

key pair

Definition: A public key and its corresponding private key.

Extended Definition: Two mathematically related keys having the property that one key can be used to encrypt a message that can only be decrypted using the other key.

Related Term(s): private key, public key

Adapted from: CNSSI 4009, Federal Bridge Certificate Authority Certification Policy 2.25

key resource

Definition: A publicly or privately controlled asset necessary to sustain continuity of government and/or economic operations, or an asset that is of great historical significance.

Related Term(s): critical infrastructure

From: NCSD glossary

keylogger

Definition: Software or hardware that tracks keystrokes and keyboard events, usually surreptitiously / secretly, to monitor actions by the user of an information system.

Related Term(s): spyware

Knowledge Management

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Manages and administers processes and tools that enable the organization to identify, document, and access intellectual capital and information content.

From: NICE Workforce Framework

L

Legal Advice and Advocacy

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain; advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

From: NICE Workforce Framework

M

machine learning and evolution

Definition: A field concerned with designing and developing artificial intelligence algorithms for automated knowledge discovery and innovation by information systems.

Adapted from: DHS personnel

macro virus

Definition: A type of malicious code that attaches itself to documents and uses the macro programming capabilities of the document's application to execute, replicate, and spread or propagate itself.

Related Term(s): virus

Adapted from: CNSSI 4009

malicious applet

Definition: A small application program that is automatically downloaded and executed and that performs an unauthorized function on an information system.

Related Term(s): malicious code

From: CNSSI 4009

malicious code

Definition: Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Extended Definition: Includes software, firmware, and scripts.

Related Term(s): malicious logic

Adapted from: CNSSI 4009. NIST SP 800-53 Rev 4

malicious logic

Definition: Hardware, firmware, or software that is intentionally included or inserted in a system to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Related Term(s): malicious code

Adapted from: CNSSI 4009

malware

Definition: Software that compromises the operation of a system by performing an unauthorized function or process.

Synonym(s): malicious code, malicious applet, malicious logic

Adapted from: CNSSI 4009, NIST SP 800-83

mitigation

Definition: The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences.

Extended Definition: Implementing appropriate risk-reduction controls based on risk management priorities and analysis of alternatives.

Adapted from: DHS Risk Lexicon, CNSSI 4009, NIST SP 800-53 Rev 4

moving target defense

Definition: The presentation of a dynamic attack surface, increasing an adversary's work factor necessary to probe, attack, or maintain presence in a cyber target.

From: DHS personnel

N

network resilience

Definition: The ability of a network to: (1) provide continuous operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged); (2) recover effectively if failure does occur; and (3) scale to meet rapid or unpredictable demands.

Adapted from: CNSSI 4009

Network Services

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Installs, configures, tests, operates, maintains, and manages networks and their

firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

From: NICE Workforce Framework

non-repudiation

Definition: A property achieved through cryptographic methods to protect against an individual or entity falsely denying having performed a particular action related to data.

Extended Definition: Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

Related Term(s): integrity, authenticity

Adapted from: CNSSI 4009; From: NIST SP 800-53 Rev 4

O

object

Definition: A passive information system-related entity containing or receiving

information.

Related Term(s): subject, access, access control

Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4

Operate & Maintain

Definition: A NICE Workforce Framework category consisting of specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.

From: NICE Workforce Framework

operational exercise

Definition: An action-based exercise where personnel rehearse reactions to an incident scenario, drawing on their understanding of plans and procedures, roles, and responsibilities.

Extended Definition: Also referred to as operations-based exercise.

Adapted from: DHS Homeland Security Exercise and Evaluation Program

Operations Technology

Definition: The hardware and software systems used to operate industrial control devices.

Related Term(s): Industrial Control System

Adapted from: DHS personnel

outside(r) threat

Definition: A person or group of persons external to an organization who are not authorized to access its assets and pose a potential risk to the organization and its assets.

Related Term(s): inside(r) threat

Adapted from: CNSSI 4009

Oversight & Development

Definition: A NICE Workforce Framework category consisting of specialty areas providing leadership, management, direction, and/or development and advocacy so that all individuals and the organization may effectively conduct cybersecurity work.

From: NICE Workforce Framework

P

passive attack

Definition: An actual assault perpetrated by an intentional threat source that attempts

to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations.

Related Term(s): active attack

Adapted from: IETF RFC 4949, NIST SP 800-63 Rev 1

password

Definition: A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

From: FIPS 140-2

pen test

Definition: A colloquial term for penetration test or penetration testing.

Synonym(s): penetration testing

penetration

Synonym(s): intrusion

penetration testing

Definition: An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Adapted from: NCSD Glossary, CNSSI 4009, NIST SP 800-53 Rev 4

Personal Identifying Information / Personally Identifiable Information

Definition: The information that permits the identity of an individual to be directly or indirectly inferred.

Adapted from: NCSD Glossary, CNSSI 4009, GAO Report 08-356, as cited in NIST SP 800-63 Rev 1

phishing

Definition: A digital form of social engineering to deceive individuals into providing sensitive information.

Adapted from: NCSD Glossary, CNSSI 4009, NIST SP 800-63 Rev 1

plaintext

Definition: Unencrypted information.

Related Term(s): ciphertext

From: CNSSI 4009

precursor

Definition: An observable occurrence or sign that an attacker may be preparing to

cause an incident.

Related Term(s): indicator

Adapted from: CNSSI 4009, NIST SP 800-61 Rev 2 (DRAFT)

Preparedness

Definition: The activities to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents.

Adapted from: NIPP

privacy

Definition: The assurance that the confidentiality of, and access to, certain information about an entity is protected.

Extended Definition: The ability of individuals to understand and exercise control over how information about themselves may be used by others.

From: NIST SP 800-130; Adapted from: DHS personnel

private key

Definition: A cryptographic key that must be kept confidential and is used to enable the operation of an asymmetric (public key) cryptographic algorithm.

Extended Definition: The secret part of an asymmetric key pair that is uniquely associated with an entity.

Related Term(s): public key, asymmetric cryptography

Adapted from: CNSSI 4009, NIST SP 800-63 Rev 1, FIPS 201-2, FIPS 140-2, Federal Bridge Certificate Authority Certification Policy 2.25

Protect & Defend

Definition: A NICE Workforce Framework category consisting of specialty areas responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks.

From: NICE Workforce Framework

public key

Definition: A cryptographic key that may be widely published and is used to enable the operation of an asymmetric (public key) cryptographic algorithm.

Extended Definition: The public part of an asymmetric key pair that is uniquely associated with an entity and that may be made public.

Related Term(s): private key, asymmetric cryptography

Adapted from: CNSSI 4009, NIST SP 800-63 Rev 1, FIPS 201-2, FIPS 140-2,

public key cryptography

Definition: A branch of cryptography in which a cryptographic system or algorithms use two uniquely linked keys: a public key and a private key (a key pair).

Synonym(s): asymmetric cryptography, public key encryption

Adapted from: CNSSI 4009, FIPS 140-2, InCommon Glossary

public key encryption

Synonym(s): public key cryptography

Public Key Infrastructure

Definition: A framework consisting of standards and services to enable secure, encrypted communication and authentication over potentially insecure networks such as the Internet.

Extended Definition: A framework and services for generating, producing, distributing, controlling, accounting for, and revoking (destroying) public key certificates.

Adapted from: CNSSI 4009, IETF RFC 2828, Federal Bridge Certificate Authority Cross-certification Methodology 3.0, InCommon Glossary, Kantara Identity

Assurance Framework 1100, NIST SP 800-63 Rev 1

Q

R

Recovery

Definition: The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.

Adapted from: NIPP

Red Team

Definition: A group authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an enterprise’s cybersecurity posture.

Related Term(s): Blue Team, White Team

Adapted from: CNSSI 4009

Red Team exercise

Definition: An exercise, reflecting real-world conditions, that is conducted as a simulated attempt by an adversary to attack or exploit vulnerabilities in an enterprise's information systems.

Related Term(s): cyber exercise

Adapted from: NIST SP 800-53 Rev 4

redundancy

Definition: Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.

From: DHS Risk Lexicon

resilience

Definition: The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

From: DHS Risk Lexicon

response

Definition: The activities that address the short-term, direct effects of an incident and may also support short-term recovery.

Extended Definition: In cybersecurity, response encompasses both automated and manual activities.

Related Term(s): recovery

Adapted from: National Infrastructure Protection Plan, NCPS Target Architecture Glossary

response plan

Synonym(s): incident response plan

risk

Definition: The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences.

Adapted from: DHS Risk Lexicon, NIPP and adapted from: CNSSI 4009, FIPS 200, NIST SP 800-53 Rev 4, SAFE-BioPharma Certificate Policy 2.5

risk analysis

Definition: The systematic examination of the components and characteristics of risk.

Related Term(s): risk assessment, risk

From: DHS Risk Lexicon

risk assessment

Definition: The product or process which collects information and assigns values to

risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making.

Extended Definition: The appraisal of the risks facing an entity, asset, system, or network, organizational operations, individuals, geographic area, other organizations, or society, and includes determining the extent to which adverse circumstances or events could result in harmful consequences.

Related Term(s): risk analysis, risk

Adapted from: DHS Risk Lexicon, CNSSI 4009, NIST SP 800-53 Rev 4

risk management
Definition: The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

Extended Definition: Includes: 1) conducting a risk assessment; 2) implementing strategies to mitigate risks; 3) continuous monitoring of risk over time; and 4) documenting the overall risk management program.

Related Term(s): enterprise risk management, integrated risk management, risk

From: DHS Risk Lexicon and Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4

risk mitigation

Synonym(s): mitigation

risk-based data management

Definition: A structured approach to managing risks to data and information by which an organization selects and applies appropriate security controls in compliance with policy and commensurate with the sensitivity and value of the data.

Adapted from: DHS personnel

rootkit

Definition: A set of software tools with administrator-level access privileges installed on an information system and designed to hide the presence of the tools, maintain the access privileges, and conceal the activities conducted by the tools.

Adapted from: CNSSI 4009

S

secret key

Definition: A cryptographic key that is used for both encryption and decryption, enabling the operation of a symmetric key cryptography scheme.

Extended Definition: Also, a cryptographic algorithm that uses a single key (i.e., a secret key) for both encryption of plaintext and decryption of ciphertext.

Related Term(s): symmetric key

Adapted from: CNSSI 4009

Securely Provision

Definition: A NICE Workforce Framework category consisting of specialty areas concerned with conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development.

From: NICE Workforce Framework

security automation

Definition: The use of information technology in place of manual processes for cyber incident response and management.

Adapted from: DHS personnel

security incident

Synonym(s): incident

security policy

Definition: A rule or set of rules that govern the acceptable use of an organization's

information and services to a level of acceptable risk and the means for protecting the organization's information assets.

Extended Definition: A rule or set of rules applied to an information system to provide security services.

Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIST SP 800-130, OASIS SAML Glossary 2.0

Security Program Management
Definition: In the NICE Workforce Framework, cybersecurity work where a person: Manages information security (e.g., information security) implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and other resources (e.g., the role of a Chief Information Security Officer).

From: NICE Workforce Framework

signature
Definition: A recognizable, distinguishing pattern.

Extended Definition: Types of signatures: attack signature, digital signature, electronic signature.

From: CNSSI 4009; Adapted from: NIST SP 800-94

situational awareness

Definition: Comprehending information about the current and developing security posture and risks, based on information gathered, observation and analysis, and knowledge or experience.

Extended Definition: In cybersecurity, comprehending the current status and security posture with respect to availability, confidentiality, and integrity of networks, systems, users, and data, as well as projecting future states of these.

Adapted from: CNSSI 4009, DHS personnel, National Response Framework

software assurance

Definition: The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner.

From: CNSSI 4009

Software Assurance and Security Engineering

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

From: NICE Workforce Framework

spam

Definition: The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Adapted from: CNSSI 4009

spillage

Synonym(s): data spill, data breach

Spoofing

Definition: Faking the sending address of a transmission to gain illegal [unauthorized] entry into a secure system.

Extended Definition: The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.

From: CNSSI 4009

spyware

Definition: Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

Related Term(s): keylogger

Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4

Strategic Planning and Policy Development

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Applies knowledge of priorities to define an entity.

From: NICE Workforce Framework

subject

Definition: An individual, process, or device causing information to flow among objects or a change to the system state.

Extended Definition: An active entity.

Related Term(s): object, access, access control

Adapted from: NIST SP 800-53 Rev 4., CNSSI 4009

Supervisory Control and Data Acquisition

Definition: A generic name for a computerized system that is capable of gathering and processing data and applying operational controls to geographically dispersed assets over long distances.

Related Term(s): Industrial Control System

Adapted from: NCSD Glossary, CNSSI 4009

supply chain

Definition: A system of organizations, people, activities, information and resources, for creating and moving products including product components and/or services from suppliers through to their customers.

Related Term(s): supply chain risk management

Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4

Supply Chain Risk Management

Definition: The process of identifying, analyzing, and assessing supply chain risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

Related Term(s): supply chain

Adapted from: DHS Risk Lexicon, CNSSD 505

symmetric cryptography

Definition: A branch of cryptography in which a cryptographic system or algorithms

use the same secret key (a shared secret key).

Adapted from: CNSSI 4009, SANS

symmetric encryption algorithm
Synonym(s): symmetric cryptography

symmetric key
Definition: A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt plaintext and decrypt ciphertext, or create a message authentication code and to verify the code.

Extended Definition: Also, a cryptographic algorithm that uses a single key (i.e., a secret key) for both encryption of plaintext and decryption of ciphertext.

Related Term(s): secret key

From: CNSSI 4009

System Administration
Definition: In the NICE Workforce Framework, cybersecurity work where a person: Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability; also manages accounts, firewalls, and patches; responsible for access control, passwords, and account creation and administration.

From: NICE Workforce Framework

system integrity

Definition: The attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Related Term(s): integrity, data integrity

From: CNSSI 4009

Systems Development

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Works on the development phases of the systems development lifecycle.

From: NICE Workforce Framework

Systems Requirements Planning

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions; provides guidance to customers about applicability of information systems to meet business needs.

From: NICE Workforce Framework

Systems Security Analysis

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Conducts the integration/testing, operations, and maintenance of systems security.

From: NICE Workforce Framework

Systems Security Architecture

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

From: NICE Workforce Framework

T

tabletop exercise

Definition: A discussion-based exercise where personnel meet in a classroom setting or breakout groups and are presented with a scenario to validate the content of plans, procedures, policies, cooperative agreements or other information for managing an incident.

Adapted from: NCSD Glossary, DHS Homeland Security Exercise and Evaluation

Program

tailored trustworthy space

Definition: A cyberspace environment that provides a user with confidence in its security, using automated mechanisms to ascertain security conditions and adjust the level of security based on the user's context and in the face of an evolving range of threats.

Adapted from: National Science and Technology Council's Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program

Targets

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.

From: NICE Workforce Framework

Technology Research and Development

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

From: NICE Workforce Framework

Test and Evaluation

Definition: In the NICE Workforce Framework, cybersecurity work where a person: Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating information technology.

From: NICE Workforce Framework

threat

Definition: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.

Extended Definition: Includes an individual or group of individuals, entity such as an organization or a nation), action, or occurrence.

Adapted from: DHS Risk Lexicon, NIPP, CNSSI 4009, NIST SP 800-53 Rev 4

threat actor

Synonym(s): threat agent

threat agent

Definition: An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Related Term(s): adversary, attacker

Adapted from: DHS Risk Lexicon

threat analysis

Definition: The detailed evaluation of the characteristics of individual threats.

Extended Definition: In the NICE Workforce Framework, cybersecurity work where a person: Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.

Adapted from: DHS personnel; From NICE Workforce Framework

threat assessment

Definition: The product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, and/or property.

Related Term(s): threat analysis

From: DHS Risk Lexicon and adapted from: CNSSI 4009, NIST SP 800-53, Rev 4

ticket

Definition: In access control, data that authenticates the identity of a client or a service and, together with a temporary encryption key (a session key), forms a credential.

Adapted from: IETF RFC 4120 Kerberos V5, July 2005; Conrad, E., Misenauer, S., & Feldman, J. (2010). CISSP® Study Guide. Burlington, MA: Syngress

traffic light protocol

Definition: A set of designations employing four colors (RED, AMBER, GREEN, and WHITE) used to ensure that sensitive information is shared with the correct audience.

Adapted from: US-CERT

Trojan horse

Definition: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

From: CNSSI 4009

U

unauthorized access

Definition: Any access that violates the stated security policy.

From: CNSSI 4009

V

virus

Definition: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Related Term(s): macro virus

Adapted from: CNSSI 4009

vulnerability

Definition: A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

Extended Definition: Characteristic of location or security posture or of design,

security procedures, internal controls, or the implementation of any of these that permit a threat or hazard to occur. Vulnerability (expressing degree of vulnerability): qualitative or quantitative expression of the level of susceptibility to harm when a threat or hazard is realized.

Related Term(s): weakness

Adapted from: DHS Risk Lexicon, CNSSI 4009, NIST SP 800-53 Rev 4

Vulnerability Assessment and Management
Definition: In the NICE Workforce Framework, cybersecurity work where a person: Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

From: NICE Workforce Framework

W

weakness
Definition: A shortcoming or imperfection in software code, design, architecture, or deployment that, under proper conditions, could become a vulnerability or contribute to the introduction of vulnerabilities.

Related Term(s): vulnerability

Adapted from: ITU-T X.1520 CWE, FY 2013 CIO FISMA Reporting Metrics

White Team

Definition: A group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of information systems.

Related Term(s): Blue Team, Red Team

Adapted from: CNSSI 4009

whitelist

Definition: A list of entities that are considered trustworthy and are granted access or privileges.

Related Term(s): blacklist

Adapted from: DHS personnel

work factor

Definition: An estimate of the effort or time needed by a potential adversary, with specified expertise and resources, to overcome a protective measure.

Adapted from: CNSSI 4009

worm

Definition: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

From: CNSSI 4009

Last Published Date:

August 2, 2017